AI-TECH-30   PATENT APPLICATION
                                                  Serial No. 09/737,306

REMARKS

Claims 1-16, 18-24, 26-69, 71-78, 83-104 and 107-117 are pending in the captioned Application in which claims 17, 25, 70, 79, 80, 81, 105 and 106 are cancelled hereby. Claims 1-81 and 83-117 are finally rejected, subject to the aforementioned cancellation of claims.

Entry of this amendment is proper under 37 C.F.R. § 1.116 because the claims as amended are allowable for the reasons set forth herein, thereby placing the Application in condition for allowance, and such action is solicited.

Independent claims 1, 24, 44, 60, 74, 83, 90 and 101 are amended hereby, and claims 50-55, 66, 67, 69, and 116-117 are amended for consistency with claim 44 or 60 or 115 from which it depends. Claims 17, 25, 70, 79, 80, 81, 105 and 106 are cancelled hereby without prejudice to their being later presented in this or in another application.

Introduction:

A well known problem with conventional electronic voting is that there is no record by which the votes stored in the electronic voting machine memory can be audited. Conventional machines may simple only cumulate vote totals or may randomize the storage of voting records so as to preserve the secrecy of each voter's vote. The desire for the ability to audit votes cast electronically and the mandate for voter anonymity are essentially in conflict.

There is no way that any error, whether arising due to a random event affecting operation of the voting machine or a systemic problem, or even an "error" introduced intentionally to affect the election outcome, can be detected or analyzed. As a result, many computer scientists and security experts, as well as ordinary voters, distrust electronic voting machines. This issue has been consistently raised in criticism of electronic voting for many years (see, e.g., P. Neumann (1993), of record) and continues today, See, e.g.,.

[1]   David Dill et al "Frequently Asked Questions about DRE Voting Systems" at
        http://www.verifiedvoting.org/drefaq.asp

[2]   Open Voting Consortium (OVC), Frequently Asked Questions (FACs), at
        http://www.openvotingconsortium.org/faq.html

[3]   Verified Voting Foundation, "E-Voting Misconceptions" at
        http://www.verifiedvoting.org/article.asp?id=2609

23

AI-TECH-30   PATENT APPLICATION
                                                     Serial No. 09/737,306

[4]   Alan Dechert's Statement at Utah State Capital, July, 2003, at

          http://www.openvotingconsortium.org/ad/alan-ut-7-13.html

[5]   M. Shamos, "Paper v. Electronic Voting Records – An Assessment," at

          http://euro.ecom.cmu.edu/people/faculty/mshamos/paper.htm#_edn1

[6]   "OVC Response to Paper v. Electronic Voting Records – An Assessment, by Michael

       Shamos" at http://gnosis.python-hosting.com/voting-project/July.2004/0240.html

Some of these even argue that a paper receipt is not sufficient, but Applicant's arrangement is
not considered. Ref. [1] specifically notes in Section 3.1 the Avante Vote-Trakker system
which embodies Applicant's arrangement and its having been certified in California.

       There is a long felt need for an electronic voting machine that overcomes the problem
arising from the lack of any auditability in an electronic voting machine. Applicant's voting
machine as claimed addresses and provides a novel and unobvious solution that provides the
ability to perform an audit of electronic voting while still protecting the anonymity of the voter.
Moreover, Applicant's claimed arrangement can not only provide confidence in the cumulative
vote totals, but can also permit an audit to be performed on a vote-by-vote basis, if desired,
while still maintaining the voter's privacy.

       The facts that California recently mandated a paper record (Ref. [4]) and national
legislation requiring a voter-verifiable paper record is now under consideration (Ref. [3])
evidences that Applicant's arrangement satisfies the long-felt need.

       Applicant's novel and unobvious arrangement employs a randomized and unique
identifier associated with each voting session and not the voter voting in that voting session.
The unique, randomized voting session identifier is associated with the record of the voter's
voting selections stored in the voting apparatus and that stored in a tangible medium that cannot
be changed by the voting machine after a voting session is completed. Because the voting
session identifier is stored with or as a part of the voting record in both the voting machine
memory and in the tangible medium, each voting record is stored in at least two separate and
independent memory devices with the voting session identifier which provides the anonymous
link by which each stored copy of the voting record can be compared against the other stored
copies thereof, thereby to allow a vote-by-vote audit, if desired.

       Examples of a suitable tangible medium include a smart card and a printed receipt.

24

AI-TECH-30   PATENT APPLICATION
                                                        Serial No. 09/737,306

Encryption and other smart card security measures are not necessary to and, even if employed, would not provide the features of Applicant's claims. Such measures are simply inapposite where a printed receipt is utilized as the tangible medium.

While smart card security measures may be desirable where a smart card is utilized, they are not necessary to Applicant's invention. Such security measures teach the making of the details of an electronic message or transaction, including the identity of the originator thereof, available for purposes of authentication, audit and reconstruction of records of transactions. Thus, smart card security teaches away from maintaining voter anonymity.

Rejections Under 35 U.S.C. §103(a):

Claims 1-32, 34, 37-60, 65-68, 71-72, 74-81 and 93-117 are finally rejected under 35 U.S.C. §103(a) as being unpatentable over EP 0419335 to Fetterman in view of "well known smart card security techniques." Claims 83-92 are not addressed in any rejection and it appears that claims "93-117" in this rejection may be a typographical error, i.e. should have been "83-117." Applicant will respond accordingly in the interest of expediting prosecution.

The rejection is overcome in part in view of the amendment of claims 1, 24, 44, 60, 74, 83, 90 and 101, is traversed as to unamended claims, and is moot as to cancelled claims 17, 25, 79, 80, 81 and 105-106.

Fetterman relates to a voting method and means for carrying out the method wherein votes cast appear to be stored in the memory of a smart card. Specifically, about 48 votes are said to be stored in 48 memory zones of the smart card in a random place so that "any identification of a particular vote position with a particular voter is impossible [because] Only the cumulated votes of a card can be analyzed...." (Translation pages 6 & 8). Fetterman describes depositing the smart card as a ballot in an "electronic ballot box" that reads the card and cumulates the vote stored therein to provide an election result. The electronic ballot box reads and cumulates the votes stored in the memory zones of the smart card and "neutralizes" the memory zones. (Translation pages 6 & 8).

An important feature of Fetterman is that plural voting records are stored in 48 zones of a smart card in a random order so that there can be no identifying link to the voting records stored on the voting machine. Only cumulated votes from the voting booths, electronic ballot

25

AI-TECH-30   PATENT APPLICATION
                                                Serial No. 09/737,306

boxes and smart cards are available for recounting. (Translation page 3, 7th paragraph & page 8, ¶4). This necessarily precludes any possibility of directly comparing a voting record stored in a voting machine with a voting record stored on the smart card, if the voting record were to be stored rather than a cumulative vote.

Thus, Fetterman lacks any way to perform a vote-by-vote audit of the operation of the electronic voting machine. There is no "audit trail." If the cumulative vote tally maintained by the voting machine or by the electronic ballot box is questioned, all that can be done is to accumulate another vote tally from the records stored on the smart cards and if the result is different, there in no way to determine which cumulative total vote is correct or whether/where a systematic error occurred.

Examiner cites and remarks on cited chapters of four separate references (referred to as Zoreda, Rankl, Allen and Dreifus) for the allegedly "well known smart card security techniques." These references are discussed below in the same order as set forth by the Examiner.

In commenting on these references, the Examiner focuses on the security aspects of smart cards which is an entirely different problem than is that addressed in the captioned application. It is noted that Applicant claims a tangible medium separate from the voting apparatus, which medium may be, e.g., a smart card or a printed receipt, and the various approaches discussed by the references in relation to smart card security simply have no applicability in relation to a printed receipt, e.g., to Applicant's tangible medium. While smart card security could be utilized, it does not address the problem of auditing votes cast on an electronic voting apparatus.

Applicant's claims recite *inter alia* a voting apparatus, voting system and/or method wherein voting is conducted on electronic apparatus wherein the voting record for each voting session is stored, however, the voting apparatus, system and/or method provides a unique identifier for each voting session which is associated with the voting record and is stored therewith, both in/by the voting apparatus, system and/or method and in a separate tangible receipt. As a result, the tangible receipt may be employed for a voting-session-by-voting-session audit of the voting records stored in/by the voting apparatus, method and/or method

26

AI-TECH-30   PATENT APPLICATION
                                      Serial No. 09/737,306

against that on the tangible receipt.

      Smart card security is concerned with the authenticity of the smart card and of the data stored therein, and is not concerned about data stored in another apparatus such as a voting machine. Smart card security has several aspects including authentication (e.g., identifying a message sender or source) and confidentiality (e.g., masking the data from unauthorized persons). Authentication relates to identifying the sender/originator of a transmission so that the source thereof is known, which is antithetical to the voting issue wherein the identity of the originator of the data (the voter) is to be protected so that each voter's vote remains anonymous. Confidentiality relates to masking the information transmitted to all except a recipient having a key that will decrypt the information. (See, e.g., Rankl, Allen)

      "Smart Cards" by Zoreda et al (herein "Zoreda") relates to card security (pages 39-45 cited) emphasizing encryption as a security feature, such as DES algorithms that may be built in to a card. Such encryption utilizes a key or secret code that is associated with a user. (E.g., pages 41-43). These keys are shared by the sender and the recipient so that the sender can use the key to encrypt information stored in the smart card memory and the recipient can use the key to decrypt the stored encrypted information (E.g., pages 43-44) and to authenticate the sender's identity. This teaches away from what Applicant claims. Nothing in Zoreda's encryption describes or suggests that both a voting record and a random identifier associated with the voting record be stored in a voting machine and also in a separate tangible medium, and that the random identifier not be associated with any user (voter), whereby separate and independent auditable records that can be cross-checked are provided.

      The challenge process described by Zoreda (page 44) is simply the sending of an encrypted test message to verify that a recipient has the proper key to decrypt the message before real information is encrypted and sent to that recipient. Challenge involves generating a random number that is encrypted using the sender's key and sent to a recipient who can only properly decrypt the encrypted random number if the recipient has been given the correct key. If the recipient returns the correct random number to the sender, then the challenge has authenticated the recipient, and real information may then be sent. Zoreda's random number is not described as being for any other purpose. Nothing in Zoreda's challenge process describes

27

AI-TECH-30   PATENT APPLICATION
                                                       Serial No. 09/737,306

or suggests that both a voting record and a random identifier associated with the voting record be stored in a voting machine and also in a separate tangible medium, and that the random identifier not be associated with any user (voter).

The digital signatures of Zoreda (page 45) are electronic equivalents to handwritten signatures for authenticating documents, i.e. to prove the identity of the sender/originator of the document, which is the opposite of the voting session identifier recited by Applicant. Zoreda's digital signatures also teach away from what Applicant claims.

Nothing in Zoreda describes or suggests that both a voting record and a random identifier associated with the voting record be stored in a voting machine and in a separate tangible medium, and that the random identifier not be associated with any user (voter).

The "Smart Card Handbook" by Rankl et al (herein "Rankl") includes a chapter 4 relating to fundamentals of information technology (pages 61-97 cited) and a chapter 8 relating to security methods (pages 237-272 cited). The Examiner refers to a statement on page 84 that "Typical applications [of random numbers] in the field of Smart Cards are ensuring the uniqueness of a session during authentication, as padding in the course of encryption or as a starting value in transmission counters." That statement is immediately preceded by the statement that "Random numbers are routinely needed as part of cryptographic procedures."

Rankl's expressly states that the random number is used only during a session and has no use thereafter. This is consistent with Rankl's other statements regarding authentication.

Rankl defies authentication as meaning that a recipient "can ensure that the received message has not been altered during transmission" (Page 66, bottom) such as by use of a message authentication code (MAC). A MAC is a value calculated by the sender from the content of a message and that is transmitted with the message wherein the recipient can likewise calculate the MAC from the message and compare the received and calculated MACs to determine if the message has been altered. (Page 84).

Thus the MAC described by Rankl has a value related to the message, and is not randomized. In addition, Rankl's authentication relates to the message content, and not to a voting session. Moreover, it is calculated and transmitted and used for authentication. It is not stored along with a voting record or as part of a voting record – it is calculated and sent, and

28

then is recalculated by recipient and is discarded once authenticity or lack thereof is
determined.

Examiner also refers to Rankl's section on dynamic cryptographic keys (page 258),
which are keys valid only for one transmission session for encrypting and decrypting messages
thereof. These keys are used for encrypting and decrypting messages, and have no apparent use
after the messages are decrypted. Nothing in Rankl describes or suggests a random identifier of
a voting session that is stored with or as part of a voting record, or that is stored in a voting
memory and in a separate tangible medium.

"Smart Cards, Seizing Strategic Business Opportunities" edited by **Allen** et al (herein
"**Allen**") includes a chapter 16 (pages 248-264 cited) relating to smart card security and
privacy. Allen defines several aspects of security – Encryption which is "the transformation of
data into a form unreadable by anyone without a secret key" (page 251 & 254) and
Authentication which is a "process that guarantees that the message received is the correct
message issued by the correct person" (page 252 & 254-55 & 258). Allen also discusses
various attacks and counterattacks that may be made against data stored in smart cards (page
260), however, these counterattacks merely set forth ways to avoid or thwart an attack and are
simply not related to the novel and unobvious voting apparatus and method recited by
Applicant's claims. They are not the same as or equivalent to a unique voting session
identifier; neither do they suggest a unique voting session identifier, or employing a unique
voting session identifier stored in voting apparatus and in a separate tangible receipt, thereby
enabling a vote that is auditable on a vote-by-vote basis.

"Smart Cards, A Guide to Building and Managing Smart Card Applications" by **Dreifus**
et al (herein "**Dreifus**") includes a chapter 9 (pages 139-156 cited) that relates to system and
data integrity. Dreifus addresses a transaction system wherein it is desirable to be able to
reconstruct each transaction in complete detail, and the important aspects include "appended
security data (date, time sequence stamps (page 141)), a transaction log, unique batch sequence
numbers (serial ID numbers (page 142), value-ratio monitoring, systemwide audit controls, off-
line processing (to reconstruct transactions (page 143)), operational rules, secure application

29

AI-TECH-30   PATENT APPLICATION
                                                               Serial No. 09/737,306

modules and storing value on the host computer." (Page 140 et seq.). All of these are directed
to identifying each of the participants to any transaction and to being able to completely trace
and reconstruct any missing data relating to any transaction and to the processing thereof.

What Dreifus describes for having complete knowledge of each transaction is the
opposite of what Applicant addresses, wherein the voting record is to be preserved and
auditable, while the identity of the voter is to be anonymous. Dreifus' sequence stamps,
transaction logs (whether electronic or paper), sequential transaction and batch numbers, and
the like, are the antithesis of a voting arrangement wherein the identity of the voter is
anonymous and private. Thus, Dreifus teaches away from what Applicant claims.

It is submitted that one skilled in the art would not be led to employ Applicant's unique
identifier unrelated to voter identity because the prior art teaches away from this feature of the
invention, e.g., at least Dreifus, Zoreda and Allen teach towards authenticating, ordering and/or
numbering the steps of a transaction so that the transaction can be reconstructed and the parties
can be identified.

It is "error to find obviousness where [the] references 'diverge from and teach away
from the invention at hand'." *In re Fine*, 5 U.S.P.Q.2d 1596, 1599 (Fed. Cir. 1988) citing *W. L.
Gore & Assoc. v. Garlock, Inc.*, 721 F.2d 1540, 1550, 220 U.S.P.Q. 303, 311 (Fed. Cir. 1983).

Even if the applied references are combined, the result of the combination is not what
Applicant claims. The combination would lack *inter alia* the randomized voting session
identifier and the associating with and/or storing thereof with a voting record. It would also
lack the storing of the voting record and voting session identifier in a memory, e.g., of a voting
machine, and in a tangible medium separate therefrom.

Accordingly, Applicant's claim 1 is patentable at least because it recites a voting
machine including:

> "a processor for processing voting information and providing a unique voting
> session identifier for each of a plurality of voting sessions, wherein the unique voting
> session identifier is unrelated to a particular voter's personal identity;
> "a display coupled for receiving voting information from said processor;
> "a voter interface for receiving voting selections made by a voter and coupling
> same to said processor, said processor providing a voting record including the voting
> selections for each voting session;

<center>30</center>

AI-TECH-30

<div align="right">

PATENT APPLICATION
Serial No. 09/737,306
</div>

"a memory coupled to said processor for storing the voting record and the unique voting session identifier for each voting session; and

"means coupled to said processor for storing the voting record and the unique voting session identifier for each voting session in a portable tangible medium separate from said memory,"

which is not described or suggested by Fetterman and/or any one or more of the other applied references, whether taken individually or properly combined.

Applicant's claim 22 is patentable at least because it recites in combination with an electronic voting machine:

"a generator of a voting session identifier for each voting session, which voting session identifier is unrelated to the personal identity of a particular voter conducting that voting session, and

"a printer providing a tangible receipt containing at least the voting record and the voting session identifier for each voting session,"

which is not described or suggested by Fetterman and/or any one or more of the other applied references, whether taken individually or properly combined.

Applicant's claim 24 is patentable at least because it recites a voting system including:

"a processor for processing voting information and providing a unique voting session identifier for each of a plurality of voting sessions, wherein the unique voting session identifier is unrelated to a particular voter's personal identity,

"a display coupled for receiving voting information from said processor,

"a voter interface for receiving voting selections made by a voter and coupling same to said processor, said processor providing the voting selections in a voting record for each voting session,

"a memory coupled to said processor for storing the voting record and the unique voting session identifier for each voting session; and

"means coupled to said processor for storing the voting record and the unique voting session identifier for each voting session in a tangible medium separate from said memory,"

which is not described or suggested by Fetterman and/or any one or more of the other applied references, whether taken individually or properly combined.

Applicant's claim 44 is patentable at least because it recites a method for voting including:

<div align="center">31</div>

AI-TECH-30

<div align="right">

PATENT APPLICATION
Serial No. 09/737,306

</div>

"providing a unique identifier for the voting session, wherein the unique voting session identifier is unrelated to a particular voter's personal identity;

"creating a voting record including the unique voting session identifier and voting selections made during the voting session;

"storing the voting record including the unique voting session identifier and the voting selections in a memory; and

"storing the voting record including the unique voting session identifier and the voting selections in a tangible medium separate from the memory,"

which is not described or suggested by Fetterman and/or any one or more of the other applied references, whether taken individually or properly combined.

Applicant's claim 60 is patentable at least because it recites a voting system including:

"a generator of a voting identifier for each voting session, wherein at least part of the voting identifier is random and is unique for each voting session, wherein the voting identifier does not reveal the identity of the voter;

"for each of the number of voters, a chip card providing a registration record and a storage medium for recording the voter's voting selections and random voting identifier, wherein said chip card has substantial memory for recording all of the voting selections of one voter and the random voting identifier;

"a chip-card reader/writer for coupling the registration information to the voting machine and for recording each voter's voting selections and random voting identifier in the storage medium of that voter's chip card after that voter's voting session is completed,"

which is not described or suggested by Fetterman and/or any one or more of the other applied references, whether taken individually or properly combined.

Applicant's claim 74 is patentable at least because it recites a storage medium encoded with instructions including:

"means for causing the computer to provide an identifier for the voting session, wherein the identifier is unique, randomized and does not identify a voter;

"means for causing the computer to create a voting record including the voting session identifier and voting selections made during the voting session;

"means for causing the computer to store the voting record including the voting session identifier and the voting selections in a memory; and

"means for causing the computer to store the voting record including the voting session identifier and the voting selections in a tangible medium separate from the memory and to cause the tangible medium to issue after the voting record including the unique voting session identifier and the voting selections is stored therein and before a next voting session,"

<div align="center">32</div>

AI-TECH-30   PATENT APPLICATION
                                                       Serial No. 09/737,306

which is not described or suggested by Fetterman and/or any one or more of the other applied

references, whether taken individually or properly combined.

Applicant's claim 83 is patentable at least because it recites an electronic voting

machine including:

> "a generator of a voting session identifier for each voting session, wherein at
> least part of the voting session identifier is random and is unique for each voting
> session, wherein the voting session identifier for each voting session is associated with
> and stored with the voting record for that voting session in the at least one memory,"

which is not described or suggested by Fetterman and/or any one or more of the other applied

references, whether taken individually or properly combined.

Applicant's claim 87 is patentable at least because it recites voting apparatus including:

> "a processor for processing voting information and providing a unique
> randomized voting session identifier for each of plural voting sessions;
> "a display coupled for receiving voting information from said processor;
> "a voter interface for receiving voting selections made by a voter and coupling
> same to said processor, said processor providing a voting record including the voting
> selections for each voting session; and
> "at least two separate and independent memory devices coupled to said
> processor for each storing the voting record and the unique randomized voting session
> identifier for each voting session, wherein one of said memory devices is decoupled
> from said processor after the voting record and the unique randomized voting session
> identifier for one voting session is stored therein and before a next voting session,"

which is not described or suggested by Fetterman and/or any one or more of the other applied

references, whether taken individually or properly combined.

Applicant's claim 89 is patentable at least because it recites in combination with an

electronic voting machine:

> "a generator of a voting session identifier for each voting session, which voting
> session identifier is unrelated to the personal identity of a particular voter conducting
> that voting session, and
> "a printer providing a printed paper containing at least the voting record and the
> voting session identifier for each voting session, wherein the printed paper is human
> readable and/or optically readable,"

which is not described or suggested by Fetterman and/or any one or more of the other applied

33

AI-TECH-30   PATENT APPLICATION
                                                        Serial No. 09/737,306

references, whether taken individually or properly combined.

  Applicant's claim 90 is patentable at least because it recites a method for voting including:

   "providing an identifier for the voting session, wherein the identifier is unique, randomized and does not identify a voter;

   "creating a voting record including the voting session identifier and voting selections made during the voting session;

   "storing the voting record including the voting session identifier and the voting selections in a memory; and

   "storing the voting record including the voting session identifier and the voting selections on a printed paper, wherein the printed paper is human readable and/or optically readable,"

which is not described or suggested by Fetterman and/or any one or more of the other applied references, whether taken individually or properly combined.

  Applicant's claim 101 is patentable at least because it recites voting apparatus including:

   "means for providing an identifier for the voting session, wherein the identifier is unique, randomized and does not identify a voter;

   "means for creating a voting record including the voting session identifier and voting selections made during the voting session;

   "means for storing the voting record including the voting session identifier and the voting selections in a memory; and

   "means for storing the voting record including the voting session identifier and the voting selections in a portable tangible medium separate from the memory;

   "wherein said means for providing and said means for creating are embodied in a set of machine readable instructions for a computer, and wherein both of said means for storing are responsive to the set of machine readable instructions for a computer,"

which is not described or suggested by Fetterman and/or any one or more of the other applied references, whether taken individually or properly combined.

  Applicant's claim 113 is patentable at least because it recites an electronic voting machine including:

   "means for providing a unique and randomized identifier for each voting session;

   "means for creating a voting record for each voting session, wherein the voting

34

record for each voting session is created during that voting session and includes the unique and randomized voting session identifier for that voting session and voting selections made during that voting session;

"means for storing the voting record including the unique and randomized voting session identifier for that voting session and the voting selections for that voting session in at least two independent memories at the end of each voting session;

"wherein each voting record including the unique and randomized voting session identifier for that voting session and the voting selections for that voting session that is stored in at least one of the at least two independent memories cannot be changed by any means included in said electronic voting machine after completion of the voting session in which the voting record is created and stored,"

which is not described or suggested by Fetterman and/or any one or more of the other applied references, whether taken individually or properly combined.

Finally, Applicant's claim 115 is patentable at least because it recites a method for voting including:

"for each of a plurality of voting sessions conducted on the voting machine:
"providing a unique and randomized voting session identifier for each one of the number of voting sessions;

"displaying during each voting session responsive to the set of machine readable computer instructions voting information for each office, referendum, and/or question;

"creating responsive to the set of machine readable computer instructions a voting record including voting selections made for each office, referendum, and/or question and the unique and randomized voting session identifier;

"storing responsive to the set of machine readable computer instructions the voting record including voting selections and the unique and randomized voting session identifier in at least two independent memories during the voting session,"

which is not described or suggested by Fetterman and/or any one or more of the other applied references, whether taken individually or properly combined.

Applicant's claims 2-16, 18-21, 23, 26-32, 34, 37-43, 45-59, 65-68, 71-72, 75-78, 84-86, 88, 91-100, 102-104, 107-112, 114 and 116-117 are patentable at least because they depend from one of patentable claims 1, 22, 24, 44, 60, 74, 83, 87, 89, 90, 101, 113 and 115.

Claims 33, 35, 36, 69-70 and 73 are rejected under 35 U.S.C. §103(a) as being

35

unpatentable over Fetterman in view of "well known smart card security techniques" and further in view of US 6,081,793 to Challener et al.

The rejection is overcome in part in view of the amendment of claims 24 and 60, is traversed as to unamended claims, and is moot as to cancelled claim 70.

Fetterman and the "well known smart card security techniques" references are discussed in detail above, which discussion is hereby incorporated herein.

Challener et al relates to a system and method for secure computer moderated voting wherein cryptographic routines are utilized in a distributed data processing system to maximize privacy of voter identity and completed ballots. (Abstract). Challener does not describe or suggest a voting apparatus or machine that may be utilized at a polling place without connection to a server or other part of a distributed data processing system, as is recited in certain of Applicant's claims.

To the extent smart cards are utilized in the Challener system, they are registration cards issued when the voter registers to vote, and are thereafter utilized for identifying registered voters for issuing the correct ballot to the voter when the voter appears to vote. (Column 2, line 61 to column 3, line 28).

Only information relating to voter identification and precinct is stored in the smart card, as is clearly illustrated in Figure 2A of Challener wherein all of the information described as stored in smart card N has to do with the voter's identity, public and private encryption keys, the voting precinct address and ballot ID for that precinct to which the voter is assigned, and a PIN for the smart card. (Column 3, lines 10-28).

No voting selections or other information relating to the voting record or to the voting session are stored in the smart card of Challener, and Challener provides no motivation and/or suggestion for doing so, either in a smart card or other tangible medium. In fact, Challener provides no motivation and/or suggestion for storing any information in a smart card at the voting precinct or polling place.

Because Challener is directed to communicating information, e.g., between a polling place and a central processing facility/servers utilizing cryptographic routines for maximizing privacy (e.g., Abstract; Figure 1), Challener is not concerned about creating an independent record at the voting machine, e.g., at the polling place.

36

Challener does not describe or suggest a tangible medium and the utilization thereof as claimed. Challener does not describe or suggest a randomized and unique voting session identifier and the utilization thereof as claimed.

As a result, Challener cannot suggest the publication of a voting record and/or its associated voting session identifier, whether via the Internet or otherwise.

One advantage of this aspect of Applicant's invention is that the voting information stored in the tangible medium cannot be changed by the voting apparatus, either through an intentional or an accidental action, after a voting session ends, and so is completely independent of the voting machine and available to provide independent authentication of the vote. A further advantage is that, where a voting session identifier is utilized, the voting record stored in the tangible medium may be compared against the voting record stored in the voting apparatus and/or voting system for verification of each vote cast. Further, where the voting session identifier is unrelated to the voter's identity (e.g., is random or randomized), such independent verification of the vote can be performed while preserving the privacy and anonymity of each voter.

Accordingly, Challener also lacks a voting session identifier and a tangible medium, also lacking in the Fetterman and smart card references, and so cannot, even if combined with the other references, supply the missing features needed to render Applicant's claims obvious.

Applicant's claims 33, 35, 36, 69-70 and 73 are patentable at least because they depend from one of patentable claims 24 and 60. In addition, claims 33, 35 and 69 relate to the publication of a voting record and/or its associated voting session identifier, whether via the Internet or otherwise, which is not described or suggested by Fetterman and/or Challener et al and/or any one or more of the other applied references, whether taken individually or in proper combination.

Claims 61-64 are rejected under 35 U.S.C. §103(a) as being unpatentable over Fetterman in view of "well known smart card security techniques" and further in view of the 1998 Advanced Card Technology Sourcebook. The rejection is respectfully traversed.

Fetterman and the allegedly "well known smart card security techniques" are discussed

AI-TECH-30   PATENT APPLICATION
                                                                       Serial No. 09/737,306

above, and such discussion is incorporated herein.

      The Sourcebook relates to the amount of memory available in a smart card.

      Applicant's claims 61-64 are patentable at least because they depend from patentable claim 60.

      Accordingly, the rejections under 35 U.S.C. §103(a) are overcome and should be withdrawn.

Formal Drawing:

      Applicant again continues his request for acknowledgment in the next paper of the acceptance of the formal drawing filed on or about April 9, 2002.

Conclusion:

      Applicant respectfully requests that this Response be entered, that claims 1-16, 18-24, 26-69, 71-78, 83-104 and 107-117 be allowed, and that the present Application be passed to issuance.

      The number of claims remaining being less than the number previously paid for, no fee is due in consequence of this timely filed response. However, should any fee be due in consequence of this response, please charge such fee and deposit any refund to Deposit Account 04-1406 of Dann, Dorfman, Herrell & Skillman.

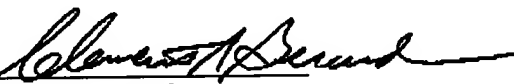AI-TECH-30   PATENT APPLICATION
                                                       Serial No. 09/737,306

The Examiner is requested to telephone the undersigned attorney if there is any question or if prosecution of this Application could be furthered by telephone.

                              Respectfully submitted,
                              Dann, Dorfman, Herrell & Skillman, P.C.
                              Attorneys for Applicant(s)

                              By: _____
                              Clement A. Berard
                              PTO Registration No. 29,613

August 24, 2004

Dann, Dorfman, Herrell and Skillman, P.C.   Telephone: 215-563-4100
1601 Market Street, Suite 2400   Facsimile: 215-563-4044
Philadelphia, PA 19103